UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,015	12/26/2000	Glenn Langford	77666-8/jpw	2269

7380 7590 07/18/2011

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P 5Y6
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
07/18/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us.mail@smart-biggar.ca

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GLENN LANGFORD

Appeal 2009-007362
Application 09/746,015
Technology Center 2400

Before JOSEPH L. DIXON, LANCE LEONARD BARRY, and
JAY P. LUCAS, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Patent Examiner rejected claims 1-11, 13-30, 33, and 35-42. The Appellant appeals therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

INVENTION

The Appellant describes the invention at issue on appeal as follows.

> Systems, methods, components are provided all for the purpose of controlling access to decryption keys needed to decrypt ciphertext. A key release agent [("KRA")] is provided which controls decryption key distribution. The key release method starts with receiving an encrypted key, key related information and decryptor information from a decryptor and determining a whether a private key corresponding to the key ciphertext is available. Upon determining the private key corresponding to the key ciphertext is available, a decision is made based on decryptor information of the decryptor and the key related information whether decryption of the key ciphertext is to be permitted. Decryptors adapted to participate with the KRA in the above described key distribution methods are also provided.

(Abstract.)

ILLUSTRATIVE CLAIM

13. A key release method comprising:

> receiving a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext from a decryptor;
>
> locating decryptor authorization logic stored externally to the decryptor with use of the key related information;
>
> obtaining decryptor information in respect of the decryptor;
>
> deciding based on the decryptor information and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted.

REJECTIONS

Claims 13-30 and 38-42 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,481,613 ("Ford").

Claims 1-11, 33, and 35-37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ford.

FINDINGS OF FACT

Ford describes its invention as "a computer network in which decryption of data is only possible when a decryptor is authorized in accordance with a set of access control attributes specified by the [associated] encryptor." (Col. 1, ll. 7-10.)

REJECTION UNDER 35 U.S.C. § 102(b)

The issue before us is whether the Examiner erred in reading both the decryptor authorization logic and the decryptor information of independent claims 13, 29, 30, and 38 on the decryptor privilege attributes of Ford.

"'[T]he main purpose of the examination, to which every application is subjected, is to try to make sure that what each claim defines is patentable. . . . [T]he name of the game is the claim. . . .'" *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) (quoting Giles S. Rich, *The Extent of the Protection and Interpretation of Claims-American Perspectives*, 21 Int'l Rev. Indus. Prop. & Copyright L. 497, 499 (1990)). Here, the Examiner construes independent claims 13, 29, 30, and 38 as not "requir[ing] the [claimed] decryptor authorization logic and the decryptor information to be separate . . . ." (Ans. 21.) Based on this premise, the Examiner finds that "Ford teaches . . . decryptor privilege attributes (decryptor information and decryptor authorization logic) . . . (column 6, lines 58-67)." (*Id.*)

We agree, however, with the Appellant's following argument.

> [T]his interpretation of the claims and prior art results in the illogical result of the decryptor authorization logic and the decryptor information having the same meaning. This is clearly an error.
>
> For example, the limitation of "deciding based on the decryptor information and the decryptor authorization logic . . . " in claim 13 would be nonsensical if these two terms [viz., decryptor information and the decryptor authorization] did not have different meanings.

(App. Br. 6.)

Therefore, we conclude that the Examiner erred in reading both the decryptor authorization logic and the decryptor information of independent claims 13, 29, 30, and 38 on the decryptor privilege attributes of Ford.

REJECTION UNDER 35 U.S.C. § 103(a)

Based on the Appellant's arguments, we will decide the appeal of claims 1-4, 6-11, and 33-37 on the basis of claim 1 alone and the appeal of claim 5 separately. *See* 37 C.F.R. § 41.37(c)(1)(vii).

The issues before us are (1) whether the Examiner erred in finding that Ford would have suggested decryptor authorization logic, as required by representative claim 1, and (2) whether the Examiner erred in finding that Ford would have suggested a decryptor providing decryptor information to a KRA while establishing a secure connection therewith, as required by claim 5.

We address the aforementioned issues *seriatim.*

CLAIMS 1-4, 6-11, AND 33-37

"[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324, (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)).

Here, we agree with that the Examiner's following claim construction is reasonable. "[T]he 'decryptor authorization logic' is stored and transmitted, as per the claims. This feature qualifies the 'decryptor authorization logic' as information used to make a decision on whether or not to release a decryption key." (Ans. 21-22.)

"Though understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not a part of the claim. For example, a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment." *SuperGuide Corp. v. DirecTV Enters, Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (citing *Electro Med. Sys. S.A. v. Cooper Life Sci., Inc.*, 34 F.3d 1048, 1054 (Fed.Cir. 1994).

Here, the Appellant makes the following argument.

> It is clearly wrong to interpret "decryptor privilege attribute information" to be analogous to "logic" that can be applied to data; as the Examiner has done . . . . On page 15 of the description of the present invention, in describing *a specific embodiment*, it is stated on lines 1-4 that: "Each access identifier is associated with a set of rules (more generally, is associated with respective decryptor authorization logic)". Clearly, a set of rules is an *example* of logic.

(App. Br. 7) (emphases added).

For our part, we will not read into the representative claim the specific embodiment from the Specification in which the broadly claimed "decryptor authorization logic" constitutes a set of rules. The Appellant is free to amend the broadly claimed "decryptor authorization logic" to "a set of decryptor authorization rules" or the like.

In view of the aforementioned claim interpretation, the Examiner makes the following findings.

> Ford teaches such information used to make a decision on releasing a decryption key. Ford teaches that the KRA will obtain decryptor privilege attribute information to verify that the requesting decryptor is authorized (column 6, lines 42-44), and that this information may be obtained by the decryptor or from a supporting (external) database (column 6, lines 53-56). This decryptor privilege information is used to make a decision (allow or disallow) on releasing the decryption key (Figure 2, step 38). This information used to make a decision is authorization logic as it is used to make a decision.

(Ans. 22.) The Appellant does not contest this finding. "Silence implies assent." *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 572 (1985).

Therefore, we conclude that the Examiner did not err in finding that Ford would have suggested decryptor authorization logic, as required by representative claim 1.

CLAIM 5

"It is not the function of [the U.S. Court of Appeals for the Federal Circuit] to examine the claims in greater detail than argued by an appellant, looking for nonobvious distinctions over the prior art." *In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991). "Similarly, it is not the

function of this Board to examine claims in greater detail than argued by an appellant, looking for distinctions over the prior art." *Ex Parte Shen*, No. 2008-0418, 2008 WL 4105791 at * 9 (BPAI Sep. 4, 2008).

Here, the Examiner makes the following "specific and detailed findings," *Ex parte Belinne*, No. 2009-004693, 2009 WL 2477843, at *4 (BPAI Aug. 10, 2009) (informative), regarding Ford.

> Ford states "the decryptor privilege attributes, which maybe supplied by the decryptor through the key release request or by the database" (column 6, lines 58-62). This passage explicitly mentions that the decryptor information is received from the decryptor, and that it can be received through the key release request. Ford then discloses that the key release request must be protected, such as by encryption, and use integrity mechanisms, such as digitally signing the request (column 7, lines 1-8), which is a secure connection as it both encrypts and repudiates the transaction. Therefore, the Examiner respectfully asserts that Ford does teach both obtaining the decryptor information from the decryptor and establishing a secure connection with the decryptor while obtaining the decryptor information.

(Ans. 23-24.)

For his part, the Appellant does not address these findings. Instead, he merely alleges that "Ford does not disclose obtaining the dccryptor information from the decryptor. Furthermore, there is no disclosure in the cited passage of establishing a secure connection with the decryptor while obtaining the decryptor information." (App. Br. 8-9.) These allegations "do not . . . explain why the Examiner's explicit fact finding is in error." *Belinne*, at *4.

Therefore, we conclude that the Examiner did not err in finding that Ford would have suggested a decryptor providing decryptor information to a

KRA while establishing a secure connection therewith, as required by claim 5.

DECISION

We reverse the rejection of claims 13, 29, 30, and 38 and of claims 14-28 and 39-42, which depend therefrom.

We affirm the rejections of claims 1 and 5 and of claims 2-4, 6-11, and 33-37, which fall with claim 1.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

llw